02DO

Docket No. 367.38672X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Olli IMMONEN

Serial No.: 09/597,982

Filed: June 19, 2000

Title: WIM MANUFACTURER CERTIFICATE

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

July 20, 2000

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on:

UK Patent Application No.(s) 9914262.2
Filed: June 18, 1999

A certified copy of said UK Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/ssr
Attachment

The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

09/597982

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

CERTIFIED COPY OF PRIORITY DOCUMENT

Signed M Conkie

Dated 26 JUN 2000

Patents Form 1/77

Patents Act
(Rule 16)

The Patent Office

20JUN99 E455801-1 002716
P01/7700.0.00 - 9914262.2

THE PATENT OFFICE
18 JUN 1999
RECEIVED BY HAND

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference

PAT 99415 GB

2. Patent application number
(The Patent Office will fill in this part)

9914262.2

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

NOKIA MOBILE PHONES LIMITED
KEILALAHDENTIE 4
02150 ESPOO
FINLAND

Patents ADP number *(if you know it)*

5911995 0047

If the applicant is a corporate body, give the country/state of its incorporation

FINLAND

4. Title of the invention

WIM Manufacturer Certificate

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

NOKIA IPR DEPARTMENT
NOKIA HOUSE
SUMMIT AVENUE
FARNBOROUGH
HAMPSHIRE
GU140NG UK

Patents ADP number *(if you know it)*

75 77638001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	4
Claim(s)	1 a
Abstract	
Drawing(s)	

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 18/6/99.

PAUL HIGGIN 18.6.99

12. Name and daytime telephone number of person to contact in the United Kingdom

Miss K Jeffery 01252 865302

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

WIM Manufacturer Certificate

Abstract

The WAP Identity module contains private keys and associated certificates. For some situations it may be useful to have certificates that are not personalised for the actual user, but can be used to create actual personal certificates. This paper introduces certificates created by a WIM manufacturer. They can be used in the registration process, to make sure that keys being certified are in a secure environment.

Document information

Author(s)	Olli Immonen
Document Version	0.1
Document Status*	Draft

* Status is defined as:
Draft – Confidential to WAP. Represents the author's views only.
WAG Draft – Confidential to WAP. Work in progress by WAG.
WAP Draft – Confidential to WAP. Work in progress by WAG. Published to all WAP members.
Public – Publicly available document.

Intellectual Property Notice

Version History

Version 0.1	17 Jun 1999	Olli Immonen	Initial revision

Introduction

The WAP Identity module contains private keys and associated certificates. For some situations it may be useful to have certificates that are not personalised for the actual user, but can be used to create actual personal certificates. This paper introduces certificates created by a WIM manufacturer. They can be used in the registration process, to make sure that keys being certified are processed in a secure environment.

The personal certificates can be stored in the WIM or in the phone, or in a directory (eg, LDAP).

References

[WAPWIM] "Wireless Application Protocol Identity Module Specification", version 0.11, 27-May-1999

[WAPWTLS] "Wireless Transport Layer Specification", version 12-Feb-1999

[X509] "The Directory – Authentication Framework", CCITT, Recommendation X.509, 1988.

Definitions, Acronyms, and Abbreviations

WIM	WAP Identity Module
RA	Registration Authority
CA	Certification Authority

Background

The WAP Identity Module (WIM) is a tamper resistant device that enables digital signatures and strong authentication of the user of the module. The WIM is based on asymmetric cryptography like RSA or ECC. The WIM contains private keys and associated certificates (containing the public keys).

In a registration procedure, the user of the WIM needs to obtain a user public key certificate for a key pair in the WIM. A user certificate means that the public key is associated with a user identity, relevant to a registration authority (RA).

The RA, in order to certify a public key, needs to be confident that the corresponding private key is contained in a secure device and handled in a secure way in all circumstances.

Security of a private-public key pair includes

- it is a good quality key pair (randomness, some algorithm specific checking done e.g. for RSA)
- no copies of the private key is left outside the WIM if the key pair was generated outside the device (this applies at least for keys used for digital signatures)
- it is not feasible to obtain the private key afterwards from the WIM

Security of the key pair needs to be guaranteed by the WIM manufacturer. If the registration is done physically (i.e., the registration officer and the user meet physically, and the officer is able to see the device), it may in some cases be possible to achieve some certainty of the device by looking at the device. This may not be sufficient. Also, it is not possible if the registration of the key takes place without a physical contact, i.e., using a remote connection.

Description of the WIM Manufacturer Certificate

To make it possible to verify the security of the key pair contained in the WIM, the WIM manufacturer certificate is used. It means that the WIM manufacturer, when generating a key pair, creates a certificate for the key pair.

The meaning of a WIM manufacturer certificate is that the WIM manufacturer guarantees that the key pair has been generated and stored in a secure way.

The WIM manufacturer certificate is signed using a manufacturer private key.

The contents of the certificate are descibed in the following tables.

Field	Content
Certificate serial number	Up to the manufacturer. Eg, the device serial number (ICC ID) combined with a key number.
Issuer	Manufacturer identification. Eg, the same value as in PKCS15TokenInfo.manufacturerID
Valid not before	Date and time of creating/storing the key and certificate
Valid not after	End of expected maximum lifetime of the device
Subject	A concatenation (stored as PrintableString) of • serial number (ICC ID), same as PKCS15TokenInfo.serialNumber • a letter (or combination of letters) indicating key usage (preceded with '-') • optionally key ordinal number (preceded with '-') Eg, 1234567890123456789-SD-2 9876543210987654-N
Public key	Public key associated with the private key in the device

Key Usage Indicator	Supported WIM Primitives with this Key	Comment
N	ComputeDigitalSignature	Non-repudiation. The WIM requires user verification (PIN) every time.
S	ComputeDigitalSignature	Digital signatures used for authentication (eg, for WTLS RSA or SSL handshake).
K	KeyAgreement	Used in ECDH handshake.
D	Decipher	Used for unwrapping a key (eg, for S/MIME decryption)

Verification of a Manufacturer certificate

As said above, a Registration authority should be able to verify the WIM manufacturer certificate. In order to do that, the RA should have access to the manufacturer CA certificate (containing the manufacturer public key). Based on that, the RA may verify the IM manufacturer certificate, and thus become convinced that the IM key that is being registered has proper security.

In practice, the manufacturer may have a single CA certificate to certify all keys, or it may have a top CA for certification of intermediate CAs that certify actual keys. The manufacturer

(top) CA may have been certified by a 3rd party CA, which makes it easier to securely distribute the manufacturer (top) CA certificates of different manufacturers

Creation of the WIM Manufacturer Certificate

There are different cases to create key pairs, and the associated methods to create manufacturer certificates.

Case 1

In this case, the key pair is generated outside the device and then saved in the device. In this case the generation procedure and saving needs to be highly secure. The advantage in this method is that the device need not support key generation, which may be demanding for a low-end device while maintaining good quality of the key. The disadvantage is that the generation procedure must be highly secure which may be administratively difficult to achieve.

The procedure of creating the key pair and manufacturer certificate is
1. create the key pair
2. save the private key in the device
3. erase all copies of the private key outside of the device
4. create the manufacturer certificate data for the public key
5. sign it with the manufacturer key
6. save the manufacturer certificate in the device

Case 2

In this case, the key pair is generated inside the device as a part of the manufacturing process.

The procedure of creating the key pair and manufacturer certificate is in this case
1. instruct the device to create the key pair
2. retrieve the public key
3. create the manufacturer certificate data
4. sign it with the manufacturer key
5. save the manufacturer certificate in the device

Case 3

In this case, the key pair is generated inside the device after the manufacturing process, when the module is already in the possession of the user. In this case, the device has an initial management key pair that has been issued an IM manufacturer certificate (created as described in the case 1 or 2). This key can only be used internally by the device to certify newly generated keys (ie, the device does not allow this key to be used for ordinary purposes).

The procedure of creating a new key pair and manufacturer certificate for that key is in this case:
1. instruct the device to create the key pair
2. instruct the device to create a certificate using the management key for signing that, and save the certificate as a manufacturer certificate

In this case the new manufacturer certificate must be accompanied with the manufacturer certificate of the management key, for verification.